IN THE SPECIFICATION

Please amend the paragraph beginning at page 27, line 12, as follows:

Other objects of the present invention, its characteristics, and merits thereof will probably become apparent from later description of embodiments of the present invention with reference to diagrams. It is to be noted that the technical term 'system' used in this description means the configuration of a logical set of a plurality of apparatus, but the ~~apparatus~~ apparatuses composing the system are not necessarily incorporated in the same physical cabinet.

Please delete line 10 on page 31 in its entirety as follows:

~~[Structure of Data Recorded on a Recording Medium]~~

Please delete line 4 on page 42 in its entirety as follows:

~~[Data Reproduction Processing]~~

Please amend the paragraph beginning at page 72, line 1, as follows:

The following description explains a variety of interfaces for connecting an information-processing apparatus such as a PC to an information-recording medium drive for mounting an information-recording medium. The description also explains typical processing to transfer data between the information-processing apparatus and the information-recording medium drive through the interfaces. Examples of the interface are the SCSI, the ~~IEEEE1394~~ IEEE1394, and the USB, whereas examples of the information-recording medium include the DVD and the CD.

Please amend the paragraph beginning at page 73, line 17, as follows:

Fig. 17 is an explanatory diagram showing processing carried out by an information-recording medium drive 510 to read out data of an encrypted content from an information-recording medium 520 and processing carried out by an information-processing apparatus 500 such as a PC to reproduce the data. It is to be noted that the information-processing apparatus 500 and the information-recording medium drive 510 each have a configuration ~~all but~~ identical with that explained earlier by referring to Fig. 2 except that the recording medium 195 and the drive 190, which are shown in Fig. 2, are not indispensably required in the information-processing apparatus 500 such as a PC but needed only in the information-recording medium drive 510. On the other hand, in the configuration shown in Fig. 17, the MPEG codec 130 and the TS-processing means 198 are not indispensably required in the information-recording medium drive 510 but needed only in the information-processing apparatus 500 such as a PC.

Please amend the paragraph beginning at page 99, line 7, as follows:

At the step S558 shown in Figs. 17 and 21, an AES decryption process applying the block key Kb1 generated at the step S556 is carried out. Only a data portion obtained as a result of an encryption process applying the block key Kb1 is subjected to this decryption process. In this typical configuration, an encrypted data portion of the data area excluding the seed (seed 1) [[521]] 631 of the first TS packet of the user data and a data area including at least the other seed (seed 2) 632 of the second TS packet of the user data are subjected to the decryption process. As described earlier, there are some patterns with regard to determination of a data area as the data portion obtained as a result of an encryption process applying the block key Kb1.

Please delete line 6 on page 104 in its entirety as follows:

~~[Applications to Other Data Structures]~~

Please amend the paragraph beginning at page 107, line 10, as follows:

Then, at a step [[652]] S652, a title unique key 1 is generated from the disc unique key and title key 1 denoted by reference numeral 672.

Please amend the paragraph beginning at page 113, line 19, as follows:

It is to be noted that, the various steps described in this specification can of course be executed sequentially along the time axis in an order of the description. However, the steps can also be executed as processes carried out concurrently or individually in accordance with the processing capacity or necessity of the apparatus to execute the steps. In addition, the technical term 'system' used in this specification means a logically set configuration including a plurality of apparatus even though the ~~apparatus~~ apparatuses do not have to be enclosed in one cabinet.

Please delete line 6 on page 114 in its entirety as follows:

~~Industrial Applicability~~

Please amend the Abstract at page 132 as shown on the following page: